A Collection of Hopf orders in KC_{p^3} in Characteristic p

Robert G. Underwood
Department of Mathematics
Department of Computer Science
Auburn University at Montgomery
Montgomery, Alabama

June 4, 2023

Contents

1. Introduction

Let p be a prime number and let K be a field of characteristic p that is complete with respect to a discrete valuation

$$\nu : K \to \mathbb{Z} \cup \{\infty\}$$

with uniformizing parameter π.

The valuation ring of K is

$$R = \{x \in K \mid \nu(x) \geq 0\}$$

with unique maximal ideal

$$\mathfrak{p} = \{x \in R \mid \nu(x) \geq 1\}$$

and units

$$U(R) = \{x \in R \mid \nu(x) = 0\}.$$

Let G denote a finite abstract group.

This talk concerns the construction of Hopf orders in $K[G]$ in the following cases:

1. G is the elementary abelian group of order p^n,

$$C_p^n = \langle g_1, g_2, \ldots, g_n \rangle,$$

$g_i^p = 1$, $1 \leq i \leq n$,

2. G is the cyclic group of order p^n,

$$C_{p^n} = \langle g_1, g_2, \ldots, g_n \rangle = \langle g_n \rangle$$

with $g_1^p = 1$, $g_i^p = g_{i-1}$, $2 \leq i \leq n$.

Much more is known in the case that G is elementary abelian. In fact, Hopf orders in $K[C_p^n]$ have been completely classified for $n = 1, 2, 3$ [TO70], [EU17], [Un22].

Moreover, on the dual side, A. Koch has given a complete classification of Hopf orders in $K[C_p^n]^*$, $n \geq 1$ [Ko17].

The situation is less clear in the case that G is cyclic, and aside from the $n = 1$ case, the classification is not complete.

A strategy has arisen in view of the progress in the elementary abeilian case: the methods used to construct Hopf orders in $K[C_p^n]$ can be adapted to construct collections of Hopf orders in $K[C_{p^n}]$.

We begin with a review of the classification results in the elementary abelian case.

Hopf orders in $K[C_p^n]$, $n = 1, 2, 3$

Theorem 1 (Tate-Oort).

Let g_1 be a chosen generator for C_p and let H be an arbitrary R-Hopf order in $K[C_p]$. Then H is of the form

$$E(i) = R\left[\frac{g_1 - 1}{\pi^i}\right]$$

for some integer $i \geq 0$.

Proof. See [EU17, Theorem 2.3]. □

To classify Hopf orders in $K[C_p^2]$, we need some preliminary notation.

Let $\wp(x) = x^p - x$ for $x \in K$.

For x, y, let $x^{[y]}$ denote the **truncated exponential**, defined as

$$x^{[y]} = \sum_{m=0}^{p-1} \binom{y}{m} (x-1)^m,$$

where $\binom{y}{m}$ is the **generalized binomial coefficient**

$$\binom{y}{m} = y(y-1)(y-2)\cdots(y-m+1)/m!$$

The truncated exponential was introduced by Elder in [El09].

A classification of R-Hopf orders in $K[C_p^2]$ can now be given as follows.

Theorem 2.

Let g_1, g_2 be a chosen basis for C_p^2, and let H be an arbitrary R-Hopf order in $K[C_p^2]$. Then H can be written in the form

$$E(i_1, i_2, \mu) = R\left[\frac{g_1 - 1}{\pi^{i_1}}, \frac{g_2 g_1^{[\mu]} - 1}{\pi^{i_2}}\right].$$

for integers $i_1, i_2 \geq 0$, where μ is an element of K that satisfies $\nu(\wp(\mu)) \geq i_2 - pi_1$.

Proof. See [EU17, Section 4]. □

Extending Theorem 2, this author was able to give a classification in the $n = 3$ case.

Theorem 3.

Let g_1, g_2, g_3 be a chosen basis for C_p^3 and let H be an arbitrary R-Hopf order in $K[C_p^3]$. Then H can be written in the form

$$E(i_1, i_2, i_3, \mu, \alpha, \beta) = R\left[\frac{g_1 - 1}{\pi^{i_1}}, \frac{g_2 g_1^{[\mu]} - 1}{\pi^{i_2}}, \frac{g_3 g_1^{[\alpha]}(g_2 g_1^{[\mu]})^{[\beta]} - 1}{\pi^{i_3}}\right],$$

for integers $i_1, i_2, i_3 \geq 0$, where μ, α, β are elements of K that satisfy $\nu(\wp(\mu)) \geq i_2 - pi_1$, $\nu(\wp(\alpha) + \wp(\mu)\beta) \geq i_3 - pi_1$ and $\nu(\wp(\beta)) \geq i_3 - pi_2$.

Proof. See [Un22, Proposition 5.4]. Note: Hopf orders of this type first appeared in a paper of Byott and Elder [BE18].

□

2. The Cyclic case: Hopf orders in $K[C_{p^2}]$

Now, we consider the cyclic cases.

Note: The $n = 1$ case has already been covered:

The cyclic group $C_p = \langle g_1 \rangle$ coincides with the elementary abelian group $C_p = \langle g_1 \rangle$.

As shown in Theorem 1, every Hopf order in $K[C_p]$ is a Tate/Oort Hopf order, which we now write as

$$A(i_1) = R\left[\frac{g_1 - 1}{\pi^{i_1}}\right],$$

for some integer $i_1 \geq 0$.

We consider the cyclic $n = 2$ case: the construction of Hopf orders in $K[C_{p^2}]$.

For $n = 2$, the strategy, as mentioned, is to convert the Hopf order in $K[C_p^2]$ to a Hopf order in $K[C_{p^2}]$.

We replace the elementary abelian group of order p^2,

$$C_p^2 = \langle g_1, g_2 \rangle, \quad g_1^p = 1, \ g_2^p = 1,$$

with the cyclic group of order p^2,

$$C_{p^2} = \langle g_1, g_2 \rangle = \langle g_2 \rangle, \quad g_1^p = 1, \ g_2^p = g_1.$$

Let $C_{p^2} = \langle g_1, g_2 \rangle = \langle g_2 \rangle$ denote the cyclic group of order p^2; $g_1^p = 1$, $g_2^p = g_1$.

Let $i_1, i_2 \geq 0$ be integers and let μ be an element of K. Let

$$A(i_1, i_2, \mu) = R\left[\frac{g_1 - 1}{\pi^{i_1}}, \frac{g_2 g_1^{[\mu]} - 1}{\pi^{i_2}}\right]$$

be a truncated exponential algebra over R.

We find conditions under which $A(i_1, i_2, \mu)$ is an R-Hopf order in $K[C_{p^2}]$.

Proposition 4.

Suppose that $\nu(\wp(\mu)) \geq i_2 - pi_1$ and $i_1 \geq pi_2$. Then $A(i_1, i_2, \mu)$ is an R-order in $K[C_{p^2}]$.

Proof. Since

$$\left(\frac{g_2 g_1^{[\mu]} - 1}{\pi^{i_2}}\right)^p = \frac{g_1 - 1}{\pi^{pi_2}} \in A(i_1),$$

an R-basis for $A(i_1, i_2, \mu)$ is

$$\left\{ \left(\frac{g_1 - 1}{\pi^{i_1}}\right)^a \left(\frac{g_2 g_1^{[\mu]} - 1}{\pi^{i_2}}\right)^b \right\}, \quad 0 \leq a, b \leq p - 1.$$

Moreover, as shown in [EU17, Proposition 3.4], $g_1^{[\mu]}$ is a unit in $A(i_1)$.

Thus,

$$K \otimes_R A(i_1, i_2, \mu) \cong K[C_{p^2}],$$

which shows that $A(i_1, i_2, \mu)$ is an R-order in $K[C_{p^2}]$.

□

Proposition 5.

Suppose that $\nu(\wp(\mu)) \geq i_2 - pi_1$ *and* $i_1 \geq pi_2$. *Then* $A(i_1, i_2, \mu)$ *is an* R*-Hopf order in* $K[C_{p^2}]$.

Proof. In view of Proposition 4, we only need to check that the Hopf maps of $K[C_{p^2}]$ restricted to $A(i_1, i_2, \mu)$, endow $A(i_1, i_2, \mu)$ with the structure of an R-Hopf algebra.

But we easily have $\varepsilon(A(i_1, i_2, \mu)) \subseteq R$. Moreover,

$$\Delta(A(i_1, i_2, \mu)) \subseteq A(i_1, i_2, \mu) \otimes A(i_1, i_2, \mu)$$

follow precisely as in the elementary abelian case, see [EU17, Proposition 3.4].

Finally, $S(A(i_1, i_2, \mu)) \subseteq A(i_1, i_2, \mu)$ since the coinverse map is

$$m(I \otimes m)(I \otimes I \otimes m) \cdots (I^{p^2-3} \otimes m)(I^{p^2-3} \otimes \Delta) \cdots (I \otimes I \otimes \Delta)(I \otimes \Delta)\Delta,$$

where $m : A(i_1, i_2, \mu) \otimes A(i_1, i_2, \mu) \to A(i_1, i_2, \mu)$ denotes multiplication in $A(i_1, i_2, \mu)$.

□

3. The Cyclic case: Hopf orders in $K[C_{p^3}]$

Let $C_{p^3} = \langle g_1, g_2, g_3 \rangle = \langle g_3 \rangle$ denote the cyclic group of order p^3; $g_1^p = 1$, $g_2^p = g_1$, $g_3^p = g_2$.

Let $i_1, i_2, i_3 \geq 0$ be integers with $i_1 \geq pi_2$. Let μ be an element of K that satisfies $\nu(\wp(\mu)) \geq i_2 - pi_1$. Let α, β be elements of K, and let $A = A(i_1, i_2, i_3, \alpha, \beta, \mu) =$

$$R\left[\frac{g_1 - 1}{\pi^{i_1}}, \frac{g_2 g_1^{[\mu]} - 1}{\pi^{i_2}}, \frac{g_3 g_1^{[\alpha]}(g_2 g_1^{[\mu]})^{[\beta]} - 1}{\pi^{i_3}}\right]$$

be a truncated exponential algebra over R.

By Proposition 5,

$$A(i_1, i_2, \mu) = R\left[\frac{g_1 - 1}{\pi^{i_1}}, \frac{g_2 g_1^{[\mu]} - 1}{\pi^{i_2}}\right].$$

is an R-Hopf order in $K[C_{p^2}]$.

We also note that $A(i_1, i_2, \mu)$ is a local ring [Ch00, (29.1) Proposition], [Ch00, (21.3) Corollary].

We want to find conditions so that A is an R-Hopf order in $K[C_{p^3}]$.

Lemma 6.
Assume the conditions $\nu(\wp(\alpha) + \wp(\mu)\beta) \geq i_3 - pi_1$, $\nu(\wp(\beta)) \geq i_3 - pi_2$. *Then* $g_1^{[\alpha]}(g_2 g_1^{[\mu]})^{[\beta]}$ *is a unit in* $A(i_1, i_2, \mu)$.

Proof. By [EU17, (2)], $g_1^{[\alpha]} g_1^{[-\alpha]} = 1$. As shown in [Un22, Lemma 4.2], $g_1^{[\pm\alpha]} \in A(i_1, i_2, \mu)$. Thus $g_1^{[\alpha]}$ is a unit in $A(i_1, i_2, \mu)$.

By [EU17, (2)],

$$(g_2 g_1^{[\mu]})^{[\beta]} (g_2 g_1^{[\mu]})^{[-\beta]} = 1 + f(g_2 g_1^{[\mu]} - 1, \beta)(g_1 - 1),$$

for some polynomial $f(x, y) \in \mathbb{F}_p[x, y]$.

Now the condition $\nu(\wp(\beta)) \geq i_3 - pi_2$ yields $\nu(\beta) \geq -i_2$, which implies that

$$f(g_2 g_1^{[\mu]} - 1, \beta)(g_1 - 1) \in A(i_1, i_2, \mu).$$

In fact,

$$f(g_2 g_1^{[\mu]} - 1, \beta)(g_1 - 1) \in \ker(\varepsilon).$$

Thus $f(g_2 g_1^{[\mu]} - 1, \beta)(g_1 - 1)$ is contained in the unique maximal ideal of $A(i_1, i_2, \mu)$.

And so, $1 + f(g_2 g_1^{[\mu]} - 1, \beta)(g_1 - 1)$ is a unit of $A(i_1, i_2, \mu)$.

Let c denote its inverse. Then

$$(g_2 g_1^{[\mu]})^{[\beta]}(g_2 g_1^{[\mu]})^{[-\beta]} c = 1.$$

Using the method of [Un22, Lemma 4.2], we obtain $(g_2 g_1^{[\mu]})^{[\pm\beta]} \in A(i_1, i_2, \mu)$. So, $(g_2 g_1^{[\mu]})^{[\beta]}$ is unit in $A(i_1, i_2, \mu)$.

□

Proposition 7.

Let $i_1, i_2, i_3 \geq 0$ be integers, let $\mu, \alpha, \beta \in K$. Assume the conditions $i_1 \geq pi_2$, $\nu(\wp(\mu)) \geq i_2 - pi_1$, $\nu(\wp(\alpha) + \wp(\mu)\beta) \geq i_3 - pi_1$, $\nu(\wp(\beta)) \geq i_3 - pi_2$, $\nu(\mu - \beta^p) \geq pi_3 - i_1$ and $i_2 \geq pi_3$. Then $A = A(i_1, i_2, i_3, \mu, \alpha, \beta)$ is an R-order in $K[C_{p^3}]$.

Proof. We have

$$\left(\frac{g_3 g_1^{[\alpha]}(g_2 g_1^{[\mu]})^{[\beta]} - 1}{\pi^{i_3}}\right)^p = \frac{g_2 g_1^{[\beta^p]} - 1}{\pi^{pi_3}}.$$

By [EU17, Proposition 2.2], the condition $\nu(\mu - \beta^p) \geq pi_3 - i_1$ implies that

$$\frac{g_1^{[\mu]} - g_1^{[\beta^p]}}{\pi^{pi_3}} \in A(i_1).$$

Ultimately, we obtain

$$\frac{g_2 g_1^{[\beta^p]} - 1}{\pi^{p i_3}} \in A(i_1, i_2, \mu),$$

since $i_2 \geq p i_3$.

Thus an R-basis for $A(i_1, i_2, i_3, \mu, \alpha, \beta)$ is

$$\left\{ \left(\frac{g_1 - 1}{\pi^{i_1}}\right)^a \left(\frac{g_2 g_1^{[\mu]} - 1}{\pi^{i_2}}\right)^b \left(\frac{g_3 g_1^{[\alpha]} (g_2 g_1^{[\mu]})^{[\beta]} - 1}{\pi^{i_3}}\right)^c \right\},$$

$0 \leq a, b, c \leq p - 1$.

By Lemma 6, $g_1^{[\alpha]}(g_2 g_1^{[\mu]})^{[\beta]}$ is a unit in $A(i_1, i_2, \mu)$.

Thus,

$$K \otimes_R A(i_1, i_2, i_3, \mu, \alpha, \beta) \cong K[C_{p^3}],$$

which shows that $A(i_1, i_2, i_3, \mu, \alpha, \beta)$ is an R-order in $K[C_{p^3}]$.

□

Proposition 8.

Let $i_1, i_2, i_3 \geq 0$ be integers, let $\mu, \alpha, \beta \in K$. Assume the conditions $i_1 \geq pi_2$, $\nu(\wp(\mu)) \geq i_2 - pi_1$, $\nu(\wp(\alpha) + \wp(\mu)\beta) \geq i_3 - pi_1$, $\nu(\wp(\beta)) \geq i_3 - pi_2$, $\nu(\mu - \beta^p) \geq pi_3 - i_1$ and $i_2 \geq pi_3$. Then $A = A(i_1, i_2, i_3, \mu, \alpha, \beta)$ is an R-Hopf order in $K[C_{p^3}]$.

Proof. In view of Proposition 7, we only need to check that the Hopf maps of $K[C_{p^3}]$ restricted to A, endow A with the structure of an R-Hopf algebra.

We easily have $\varepsilon(A) \subseteq R$.

We have to work a bit harder to show that

$$\Delta(A) \subseteq A \otimes A.$$

Let

$$Q(x,y) = ((x+y+xy)^p - x^p - y^p - (xy)^p)/p.$$

Then $Q(x,y) \in (x,y)^p \subseteq \mathbb{Z}[x,y]$ with $Q(x,y)^2 \in (x^p, y^p)$.

Let

$$X = (g_1 - 1)/\pi^{i_1} \otimes 1, \quad Y = 1 \otimes (g_1 - 1)/\pi^{i_1},$$

$$T = (g_2 - 1) \otimes 1, \quad V = 1 \otimes (g_2 - 1).$$

Let

$$D = (1+T)(1+V)(1+\pi^{i_1}X)^{[\mu]}(1+\pi^{i_1}Y)^{[\mu]}.$$

By [Un22, Lemma 4.3]

$$\begin{aligned}
&((1+T)(1+V)((1+\pi^{i_1}X)(1+\pi^{i_1}Y))^{[\mu]})^{[\beta]} \\
&\qquad = \quad ((1+T)(1+V)(1+\pi^{i_1}X)^{[\mu]}(1+\pi^{i_1}Y)^{[\mu]})^{[\beta]} \\
&\qquad\qquad \cdot (1+\wp(\mu)\beta Q(\pi^{i_1}X,\pi^{i_1}Y)) \\
&\qquad\qquad\quad \cdot (1+\wp(\beta)Q(D-1,\wp(\mu)Q(\pi^{i_1}X,\pi^{i_1}Y))) \\
&+ f(\pi^{i_1}X,\pi^{i_1}Y,T,V,\mu,\alpha)\pi^{i_1}X + g(\pi^{i_1}X,\pi^{i_1}Y,T,V,\mu,\alpha)\pi^{i_1}Y
\end{aligned}$$

for polynomials $f, g \in \mathbb{F}_p[X, Y, T, V, \mu, \beta]$.

We have

$$\begin{aligned}
&+ f(\pi^{i_1}X,\pi^{i_1}Y,T,V,\mu,\alpha)\pi^{i_1}X + g(\pi^{i_1}X,\pi^{i_1}Y,T,V,\mu,\alpha)\pi^{i_1}Y \\
&\in \pi^{i_3}(A(i_1,i_2,\mu)\otimes A(i_1,i_2,\mu)).
\end{aligned}$$

Ultimately, we obtain

$$\Delta(g_3 g_1^{[\alpha]}(g_2 g_1^{[\mu]})^{[\beta]} - 1) \in \pi^{i_3} A \otimes A.$$

Thus

$$\Delta(A) \subseteq A \otimes A.$$

Finally, $S(A) \subseteq A$ since the coinverse map is

$$m(I \otimes m)(I \otimes I \otimes m) \cdots (I^{p^3-3} \otimes m)(I^{p^3-3} \otimes \Delta) \cdots (I \otimes I \otimes \Delta)(I \otimes \Delta)\Delta,$$

where $m : A \otimes A \to A$ is multiplication in $A(i_1, i_2, \mu)$.

□

4. From Characteristic p to characteristic 0

Let p be a prime number, let K be a field of characteristic p that is complete with respect to a discrete valuation

$$\nu : K \to \mathbb{Z} \cup \{\infty\}.$$

Let R denote the valuation ring with π the uniformizing parameter.

Let $C_p = \langle g_1 \rangle$ denote the cyclic group of order p.

Let $i_1 \geq 0$ be an integer. Then

$$A(i_1) = R\left[\frac{g_1 - 1}{\pi^{i_1}}\right]$$

is an R-Hopf order in $K[C_p]$.

Proposition 9.

Let $i_1 \geq 0$ be the integer as before. Let $\mathbb{Q}_p$ denote the field of p-adic rationals. Then there exists a finite field extension $L/\mathbb{Q}_p$ with valuation ring $\mathcal{O}_L$ and uniformizing parameter λ, for which

$$A(i_1) = \mathcal{O}_L \left[\frac{g_1 - 1}{\lambda^{i_1}} \right]$$

is an $\mathcal{O}_L$-Hopf order in $L[C_p]$.

Proof. Choose $r \geq 1$ so that

$$p^{r-1} \geq i_1 \geq 0,$$

and let $L = \mathbb{Q}_p(\zeta_{p^r})$, $\lambda = \zeta_{p^r} - 1$,
Then $\nu(p) = e = p^{r-1}(p-1)$, $\nu(\zeta_p - 1) = e' = e/(p-1) = p^{r-1}$.

Thus $A(i_1)$ is a (characteristic 0) $\mathcal{O}_L$-Hopf order in $L[C_p]$.

□

Next, let $i_1, i_2 \geq 0$ be integers with $i_1 \geq pi_2$. Assume that $p \mid i_2$.

Let $t \geq 0$ be so that

$$0 \geq t + i_2/p - i_1.$$

Let

$$\mu = \pi^{t+i_2/p-i_1} \in K.$$

Then $\nu(\wp(\mu)) \geq i_2 - pi_1$.

Let $C_{p^2} = \langle g_1, g_2 \rangle$, $g_1^p = 1$, $g_2^p = g_1$ denote the cyclic group of order p^2.

By Proposition 5

$$A(i_1, i_2, \mu) = R\left[\frac{g_1 - 1}{\pi^{i_1}}, \frac{g_2 g_1^{[\mu]} - 1}{\pi^{i_2}}\right]$$

is an R-Hopf order in $K[C_{p^2}]$.

Now, let $r \geq 1$ be so that

$$p^{r-1} \geq i_1 + i_2.$$

Let $L = \mathbb{Q}_p(\zeta_{p^r})$, with valuation ring $\mathcal{O}_L$ and uniformizing parameter $\lambda = \zeta_{p^r} - 1$.

Let

$$\alpha = \lambda^{t+i_2/p-i_1} \in L.$$

Proposition 10.

$$A(i_1, i_2, \alpha) = \mathcal{O}_L \left[\frac{g_1 - 1}{\lambda^{i_1}}, \frac{g_2 g_1^{[\alpha]} - 1}{\lambda^{i_2}} \right]$$

is an $\mathcal{O}_L$-Hopf order in $L[C_{p^2}]$.

Proof. Let

$$u = \zeta_p^{[\alpha]} = \sum_{m=0}^{p-1} \binom{\alpha}{m} (\zeta_p - 1)^m.$$

Then

$$\nu(1-u) \geq p^{r-1} + \nu(\alpha) \geq i_1' + i_2/p,$$

$i_1' = p^{r-1} - i_1$.

Since $p^{r-1} \geq i_1 + i_2$,

$$i_1' + i_2/p \geq i_1'/p + i_2.$$

So, by a well-known result,

$$\mathcal{O}_L\left[\frac{g_1-1}{\lambda^{i_1}}, \frac{g_2 a_u - 1}{\lambda^{i_2}}\right].$$

is an $\mathcal{O}_L$-Hopf order in $L[C_{p^2}]$.

Here, $a_u = \sum_{m=0}^{p-1} u^m e_m$ is the familiar Greither quantity.

Now by a "translation" result of Elder and U. [EU23],

$$\mathcal{O}_L\left[\frac{g_1-1}{\lambda^{i_1}}, \frac{g_2 g_1^{[\alpha]} - 1}{\lambda^{i_2}}\right] = \mathcal{O}_L\left[\frac{g_1-1}{\lambda^{i_1}}, \frac{g_2 a_u - 1}{\lambda^{i_2}}\right].$$

□

Note: We can write a_u as

$$a_u = G(g_1, u),$$

where

$$G(x, y) = \frac{1}{p} \sum_{m=0}^{p-1} \sum_{n=0}^{p-1} \zeta_p^{-mn} x^m y^n$$

is the **Gauss sum**.

5: From Characteristic 0 to characteristic p

Let L be a finite field extension of $\mathbb{Q}_p$. Assume that $\zeta_{p^3} \in L$.

We have the following result from [Un08, Theorem 3.2]:

Theorem 11 (U).

Let $i_1, i_2, i_3 \geq 0$ be integers and let u, v, w be units of $\mathcal{O}_L$. Suppose that

(i) $\nu(1-u) \geq i_1' + i_2/p$

(ii) $\nu(1-w) \geq i_2' + i_3/p$

(iii) $\nu(v^p - G(u^{-p}, w)) \geq pi_1' + i_3$,

(iv) $\nu(1-v) \geq i_1' + (i_3/p^2)$,

(v) $i_1 \geq p i_2$,

(vi) $i_2' > p i_1'$,

(vii) $i_3' \geq p^2 i_1'$,

(viii) $i_2 \geq p^2 i_3$,

(ix) $e' \geq i_1 + i_2 + i_3$.

Then

$$\mathcal{O}_L\left[\frac{g_1 - 1}{\lambda^{i_1}}, \frac{g_2 G(g_1, u) - 1}{\lambda^{i_2}}, \frac{g_3 G(g_1, v) G(g_2 G(g_1, u), w) - 1}{\lambda^{i_3}}\right]$$

is an (iterated Gauss sum) $\mathcal{O}_L$*-Hopf order in* $L[C_{p^3}]$.

□

Let

$$\mu = \frac{1}{1-\zeta_p}\sum_{m=1}^{p-1}\frac{(1-u)^m}{m}, \quad \beta = \frac{1}{1-\zeta_p}\sum_{m=1}^{p-1}\frac{(1-w)^m}{m},$$

$$\alpha = \frac{1}{1-\zeta_p}\sum_{m=1}^{p-1}\frac{(1-v)^m}{m}.$$

Note: these quantities are **truncated logarithms**.

Then conditions (i)-(ix) yield the conditions:

$\nu(\wp(\mu)) \geq i_2 - pi_1,$
$\nu(\wp(\beta)) \geq i_3 - pi_2,$
$\nu(\wp(\alpha) + \wp(\mu)\beta) \geq i_3 - pi_1,$
$\nu(\mu - \beta^p) \geq pi_3 - i_1.$

Thus by Proposition 8,

$$R\left[\frac{g_1-1}{\pi^{i_1}}, \frac{g_2 g_1^{[\mu']}-1}{\pi^{i_2}}, \frac{g_3 g_1^{[\alpha']}(g_2 g_1^{[\mu']})^{[\beta']}-1}{\pi^{i_3}}\right]$$

is an R-Hopf order in $K[C_{p^3}]$. where μ', β', α' are appropriately chosen elements in K. (K has characteristic p.)

Characteristic 0 is special

Let $L = \mathbb{Q}_p(\zeta_{p^2})$, $G = C_{p^2}$.

Then the dual of the Hopf order $\mathcal{O}_L[C_{p^2}]$ is the $\mathcal{O}_L$-Hopf order in $L[C_{p^2}]$ of the form

$$\mathcal{O}_L\left[\frac{g_1 - 1}{\lambda^{e'}}, \frac{g_2 a_w - 1}{\lambda^{e'}}\right]$$

with $w = \zeta_{p^2}^{-1}$, $e' = \nu(p)/(p-1) = p$ [UC06, Theorem 1.2].

Let

$$\omega = \frac{1}{1-\zeta_p}\sum_{m=1}^{p-1}\frac{(1-w)^m}{m}.$$

Then

$$\mathcal{O}_L\left[\frac{g_1-1}{\lambda^{e'}},\frac{g_2a_w-1}{\lambda^{e'}}\right]=\mathcal{O}_L\left[\frac{g_1-1}{\lambda^{e'}},\frac{g_2g_1^{[\omega]}-1}{\lambda^{e'}}\right]$$

Yet

$$\mathcal{O}_L\left[\frac{g_1-1}{\lambda^{e'}},\frac{g_2g_1^{[\omega]}-1}{\lambda^{e'}}\right]$$

cannot correspond to a Hopf algebra in characteristic p since $pe' \not\leq e'$.

The plan is to recast the results of [Un08] using the methods of [EU17] and [Un22], adapted to characteristic 0.

From [Ch00, Proposition (31.10)], we have

Proposition 12 (Childs).

Suppose $pi_1 \geq i_2$*, let* $u \in U(\mathcal{O}_L)$ *with* $\nu(u^p - 1) \geq pi_1' + i_2$*. Then*

$$\Delta(G(g_1, u)) = G(g_1 \otimes g_1, u) \equiv G(g_1, u) \otimes G(g_1, u)$$

modulo $\lambda^{i_2} A(i_1) \otimes A(i_1)$*.*

Childs' result can be generalized to iterated Gauss sums.

Proposition 13.

Let $u, w \in U(\mathcal{O}_L)$ *with* $\nu(G(u^p, w) - 1) \geq pi_1' + i_3$*. Then*

$\Delta(G(g_2 G(g_1, u), w))$

$= G((g_2 \otimes g_2)G(g_1 \otimes g_1, u), w) \equiv G(g_2 G(g_1, u) \otimes g_2 G(g_1, u), w)$

modulo $\lambda^{i_3} A(i_1, i_2, u) \otimes A(i_1, i_2, u)$*.*

Proposition 13 is the first step in a simplified construction of iterated Gauss sum Hopf orders in $K[C_{p^3}]$.

References

- [BE18] N. Byott, G. G. Elder, Sufficient conditions for large Galois scaffolds, *J. Num. Theory*, **182**, 2018, 95-130.
- [Ch00] L. N. Childs, Taming Wild Extensions: Hopf Algebras and Local Galois Module Theory, American Mathematical Society, Mathematical Surveys and Monographs **80**, 2000.
- [El09] G. G. Elder, Galois scaffolding in one-dimensional elementary abelian extensions, *Proc. Amer. Math. Soc.*, **137**(4), (2009), 1193-1203.
- [EU17] G. G. Elder, R. G. Underwood, Finite group scheme extensions, and Hopf orders in KC_p^2 over a characteristic p discrete valuation ring, *New York J. Math.*, **23**, 2017, 11-39.
- [EU23] G. G. Elder, R. G. Underwood, *personal communication*.
- [Ko17] A. Koch, Primitively generated Hopf orders in characteristic p, *Comm. Alg.*, **45**(6), 2017, 2673-2689.

[TO70] J. Tate, F. Oort, Group schemes of prime order, *Ann. Sci. Ec. Norm. Sup.*, **3**, (1970), 1-21.

[UC06] R. G. Underwood, L. N. Childs, Duality for Hopf orders, *Trans. Amer. Math. Soc.*, **358**(3), (2006), 1117-1163.

[Un08] R. G. Underwood, Realizable Hopf orders in KC_{p^3}, *J. Algebra*, **319**, (2008), 4426-4455.

[Un22] R. Underwood, Hopf orders in $K[C_p^3]$ in characteristic p, *J. Algebra*, **595**, (2022), 523-550.